WHAT IS CLAIMED IS:

1. For use in a system-on-a-chip (SoC) having a secure execution environment (SEE) containing secure memory, a cryptographic accelerator, comprising:

a key register located within said SEE and coupled to said secure memory to receive a cryptographic key therefrom; and

data input and output registers located outside of said SEE and coupled to said key register to allow said cryptographic key to be applied to input data arriving via said data input register to yield output data via said data output register.

2. The cryptographic accelerator as recited in Claim 1 wherein a secure data bus coupling said key register and said secure memory is isolated from external pins of said SoC.

3. The cryptographic accelerator as recited in Claim 1 wherein a cryptographic block coupled to said key register and said data input and output registers is selected from the group consisting of:

a Data Encryption Standard (DES) block, and

a triple Data Encryption Standard (3DES) block.

4. The cryptographic accelerator as recited in Claim 1 wherein said key register is a write-only register and writeable only when a central processing unit of said SoC is in a secure state.

5. The cryptographic accelerator as recited in Claim 1 wherein a data bus coupled to said input and output registers is further coupled to external pins of said SoC.

6. The cryptographic accelerator as recited in Claim 1 wherein a central processing unit mediates movement of said input data and said output data between said input and output registers and memory external to said SoC.

7. The cryptographic accelerator as recited in Claim 1 wherein said secure memory comprises secure read-only memory and secure static random-access memory.

8. A method of performing cryptography in a system-on-a-chip (SoC) having a secure execution environment (SEE) containing secure memory, comprising:

loading a key register located within said SEE with a cryptographic key from said secure memory, said key register forming a part of a cryptographic accelerator; and

applying said cryptographic key to input data arriving via a data input register to yield output data via a data output register, said data input and output registers located outside of said SEE.

9. The method as recited in Claim 8 wherein a secure data bus coupling said key register and said secure memory is isolated from external pins of said SoC.

10. The method as recited in Claim 8 wherein said applying is carried out in a cryptographic block coupled to said key register and said data input and output registers, said cryptographic block selected from the group consisting of:

a Data Encryption Standard (DES) block, and

a triple Data Encryption Standard (3DES) block.

11. The method as recited in Claim 8 wherein said key register is a write-only register and writeable only when a central processing unit of said SoC is in a secure state.

12. The method as recited in Claim 8 wherein a data bus coupled to said input and output registers is further coupled to external pins of said SoC.

13. The method as recited in Claim 8 further comprising mediating movement of said input data and said output data between said input and output registers and memory external to said SoC with a central processing unit.

14. The method as recited in Claim 8 wherein said secure memory comprises secure read-only memory and secure static random-access memory.

15. A system-on-a-chip (SoC), comprising:

a central processing unit;

a secure memory coupled to said central processing unit (CPU) and including:

secure read-only memory (ROM), and

secure static random-access memory (SRAM), said CPU and said secure memory configured to provide a secure execution environment (SEE); and

a cryptographic accelerator, including:

a key register located within said SEE and coupled to said secure memory to receive a cryptographic key therefrom, and

data input and output registers located outside of said SEE and coupled to said key register to allow said cryptographic key to be applied to input data arriving via said data input register to yield output data via said data output register.

16. The SoC as recited in Claim 15 wherein a secure data bus coupling said key register and said secure memory is isolated from external pins of said SoC.

17. The SoC as recited in Claim 15 wherein a cryptographic block coupled to said key register and said data input and output registers is selected from the group consisting of:

a Data Encryption Standard (DES) block, and

a triple Data Encryption Standard (3DES) block.

18. The SoC as recited in Claim 15 wherein said key register is a write-only register and writeable only when said CPU is in a secure state.

19. The SoC as recited in Claim 15 wherein a data bus coupled to said input and output registers is further coupled to external pins of said SoC.

20. The SoC as recited in Claim 15 wherein said CPU mediates movement of said input data and said output data between said input and output registers and memory external to said SoC.